(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2003008567 A

(43) Date of publication of application: 10.01.03

(51) Int. Cl H04L 9/10
G06F 12/14
H04L 9/08

(21) Application number: 2001184988

(22) Date of filing: 19.06.01

(71) Applicant: MATSUSHITA ELECTRIC IND CO LTD

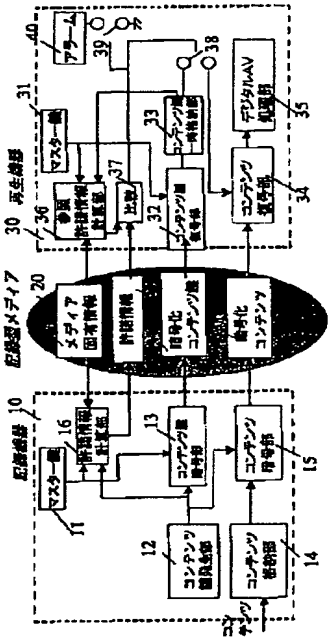
(72) Inventor: TATEBAYASHI MAKOTO
MATSUZAKI NATSUME
HARADA TOSHIHARU

(54) COPYRIGHT PROTECTION SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a copyright protection system that has a contrivance of surely inspecting whether or not a contents key obtained by decoding at a reproducing device is a substantial value.

SOLUTION: In cases where contents are encrypted with an encryption key of a media bind and stored in recording media, a unidirectional function value of the medium key, media particular information and the contents key is calculated and stored in the media, and a reproduction side conducts the similar calculation and compares both the results. A reproduction device can raise attention to a user by ringing the alarm on the basis of the discrimination result.



第１の実施例の構成図

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開２００３－８５６７
(P２００３－８５６７A)
(43) 公開日 平成15年1月10日(2003.1.10)

(51)Int.Cl.[7]		識別記号	F I			テーマコード(参考)
H04L	9/10		G06F	12/14	320 B	5B017
G06F	12/14	320			320 E	5J104
			H04L	9/00	621 A	
H04L	9/08				601 A	
					601 C	

審査請求 未請求 請求項の数 4 OL (全 12 頁)

(21) 出願番号 特願2001-184988(P2001-184988)

(22) 出願日 平成13年6月19日(2001.6.19)

(71) 出願人 000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72) 発明者 館林 誠
大阪府門真市大字門真1006番地 松下電器産業株式会社内

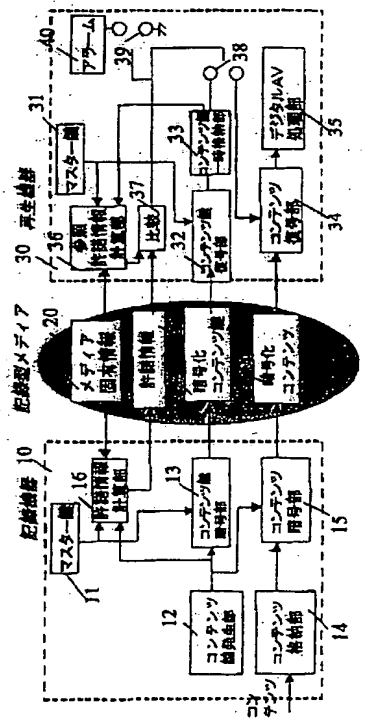
(72) 発明者 松崎 なつめ
大阪府門真市大字門真1006番地 松下電器産業株式会社内

(74) 代理人 100090446
弁理士 中島 司朗

最終頁に続く

(54)【発明の名称】著作権保護システム

(57)【要約】
【課題】 従来のメディアバインドの著作権保護システムでは、復号されたコンテンツ鍵が本来正しいものであるか否かのチェックが全く行われていない。従って、不正にコピーされた記録型メディアが装着されたときに、コンテンツ復号に先立って確実にアラームを鳴らすなどのユーザの注意を喚起するための措置をとることが困難であった。
【解決手段】 メディアバインドの暗号鍵によりコンテンツを暗号化して記録型メディアに格納する際に、メディア鍵とメディア固有情報とコンテンツ鍵の一方向性関数値を計算してメディアに格納し、再生側でも同様の計算を行い比較する。判定結果により再生機器でアラームの鳴動などユーザへの注意喚起が可能となる。



第１の実施例の構成図

1

【特許請求の範囲】

【請求項１】　デジタルコンテンツを暗号化し暗号化コンテンツとして後述する記録型メディアに記録する記録機器と、メディア固有情報により一意的に識別され暗号化コンテンツを記録する記録型メディアと、記録型メディアに格納されている暗号化コンテンツを読み出して復号化しコンテンツを取り出して再生する再生機器からなり、

上記記録機器は記録機器および再生機器に共通の秘密であるマスター鍵と、デジタルコンテンツを暗号化するときに用いるコンテンツ鍵と、上記マスター鍵でコンテンツ鍵を暗号化し暗号化コンテンツ鍵を作成するコンテンツ鍵暗号部と、デジタルコンテンツを上記コンテンツ鍵を用いて暗号化し暗号化コンテンツを作成するコンテンツ暗号部と、

記録型メディアから読み出したメディア固有情報と、上記マスター鍵と、上記コンテンツ鍵とを入力とする一方向性関数値を計算して許諾情報とする許諾情報計算部と、上記暗号化コンテンツ鍵と上記暗号化コンテンツと上記許諾情報を記録型メディアに記録する書き込み部を備え、

上記記録型メディアは上記許諾情報と上記暗号化コンテンツ鍵と上記暗号化コンテンツを記録し、

上記再生機器は、記録型メディアより暗号化コンテンツ鍵と暗号化コンテンツと許諾情報を読み出す読み出し部と、記録機器および再生機器に共通の秘密であるマスター鍵と、記録型メディアから読み込んだ暗号化コンテンツ鍵を上記マスター鍵を用いて復号しコンテンツ鍵を出力するコンテンツ鍵復号部と、記録型メディアから読み出したメディア固有情報と、上記マスター鍵と、上記コンテンツ鍵を入力として上記一方向性関数値を計算して参照許諾情報を作成する参照許諾情報計算部と、参照許諾情報と、記録型メディアから読み出した許諾情報を比較し、一致したときのみディスクから読み出した暗号化コンテンツを上記コンテンツ鍵を用いて復号を行ってコンテンツを取り出すことを特徴とする著作権保護システム。

【請求項２】　機器固有鍵を保持し、デジタルコンテンツを暗号化し後述する記録型メディアに記録する記録機器と、メディア固有情報により一意的に識別され暗号化デジタルコンテンツを記録する記録型メディアと、機器固有鍵を保持し、記録型メディアに格納されている暗号化コンテンツを読み出して復号化しコンテンツを取り出す再生機器からなり、

上記記録型メディアはさらに、メディア鍵データを予め記録し、

上記記録機器はさらに、記録型メディアから上記メディア鍵データを読み出し、機器固有鍵を用いてメディア鍵を取り出すメディア鍵計算部と、デジタルコンテンツを暗号化するときに用いるコンテンツ鍵と、上記メディア鍵でコンテンツ鍵を暗号化し暗号化コンテンツ鍵を作成するコンテンツ鍵暗号部と、デジタルコンテンツを上記コンテンツ鍵を用いて暗号化し暗号化コンテンツを作成するコンテンツ暗号部と、

記録型メディアから読み出したメディア固有情報と、上記メディア鍵と、上記コンテンツ鍵とを入力とする一方向性関数値を計算して許諾情報とする許諾情報計算部部と、上記暗号化コンテンツ鍵と上記暗号化コンテンツと上記許諾情報を記録型メディアに記録する書き込み部を備え、

上記記録型メディアはさらに許諾情報と暗号化コンテンツ鍵と暗号化コンテンツを記録し、

上記再生機器はさらに、記録型メディアから上記メディア鍵データを読み出し、機器固有鍵を用いてメディア鍵を取り出すメディア鍵計算部と、記録型メディアよりメディア固有情報と、メディア鍵データと、暗号化コンテンツ鍵と暗号化コンテンツと許諾情報を読み出す読み出し部と、記録型メディアから読み込んだ暗号化コンテンツ鍵を上記メディア鍵を用いて復号しコンテンツ鍵を出力するコンテンツ鍵復号部と、記録型メディアから読み出したメディア固有情報と、上記メディア鍵と、上記コンテンツ鍵を入力として上記一方向性関数値を計算して参照許諾情報を作成する参照許諾情報計算部と、参照許諾情報と、記録型メディアから読み出した許諾情報を比較し、一致したときのみディスクから読み出した暗号化コンテンツを上記コンテンツ鍵を用いて復号を行ってコンテンツを取り出すことを特徴とする著作権保護システム。

【請求項３】　前記メディア鍵データは、メディア鍵と機器固有鍵と、機器無効化情報から算出されるものであり、前記機器無効化情報に対応した機器固有鍵を保持している機器においては、前記メディア鍵計算部から前記メディア鍵が出力されないことを特徴とする請求項２記載の著作権保護システム。

【請求項４】　暗号化コンテンツ鍵と暗号化コンテンツは、許諾情報とは異なるメディアに記録することを特徴とする請求項１または２記載の著作権保護システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、映画などの著作物であるコンテンツをデジタル化したデータをデジタル光ディスクなどの大容量メディアに記録し、再生するシステムに関し、特に著作物が著作権者の許可なくコピーされないようにする著作権保護システムに関する。

【０００２】

【従来の技術】近年，デジタル通信、処理、蓄積技術の発展に伴ない、映画などのコンテンツ著作物をデジタル化して放送し、これを受信したユーザがこのデジタルコンテンツを，例えば記録型光ディスク等のメディアに格納し、これをデジタル再生装置で再生して楽しむという

システムが普及しつつある。こうしたシステムが普及するためには，コンテンツの著作権が保護され，著作権者との合意による制限の下でのみコンテンツの複製や再生が行われる必要となる。

【０００３】記録メディア上のデジタル著作物を著作権者の許可を受けないコピー等から保護するための一般的なシステムは，デジタルコンテンツを，ある暗号化鍵により暗号化し，ディスクに記録し，該当する復号鍵を持つ端末だけがこれを復号できるといった仕組みを備えている．そして復号装置の製造業者がそのような復号鍵を入手するためには復号装置の製造業者と著作権者との間で著作権保護に対する規定が取り決められ、製造業者はその遵守が義務付けられるというものである．同様に、暗号装置の製造業者がそのような暗号鍵を入手するためにも著作権者との間で著作権保護に対する規定が取り決められ、製造業者はその遵守が義務付けられるというものである。

【０００４】一方、光ディスクなどの記録メディア上のデータを読み出し、書き込む方法は秘密にはされないことが一般的である。このため、光ディスクなどの記録メディア上のデータはパソコンなどにより容易に読み出され、他の光ディスクにコピーされてしまう。

【０００５】従って、上記のようなデジタル著作物のコピーを保護するシステムは、メディア上のデータを他のメディアにコピーするという、通常のユーザが行い得る行為に対して有効な著作権保護の機能があるものでなければならない。

【０００６】このような著作権保護システムとして従来考案されているものを大別するとデバイスバインドと呼ばれるものとメディアバインドと呼ばれるものがある。

【０００７】デバイスバインドと呼ばれるものは、ある記録機器においてある記録メディアに記録されたデジタルコンテンツはその記録機器と通常は物理的に一体化されている再生機器でのみ再生できる、というものである（このような機器を記録再生機器という）。このようにすると、仮に記録メディア上のデータがパソコンなどにより丸ごとコピーされたとしても、コピーされた情報を再生できるのはその記録再生機器だけであり、実質的に不正コピーの被害が生じないことを意図するものである。この方法を実現するには、記録再生機器に固有のID（識別情報）があり、ディスクに記録されるコンテンツはこのIDの秘密関数値である暗号鍵により暗号化されて記録メディアに記録される。そして、同じIDの秘密関数値である復号鍵により復号化される。ここで暗号アルゴリズムとして、アルゴリズムが秘密の共通鍵暗号を用いる場合には、上記IDをそのまま暗号鍵としたり、上記IDの一方向関数値を暗号鍵としても安全性は保たれる。一方、暗号アルゴリズムとしてDESのようなアルゴリズムが公開の共通鍵暗号を用いる場合には、予め暗号復号装置には秘密のデータ値Kが暗号復号鍵として割り当てられており、実際の暗号鍵は上記データ値Kと上記IDの排他的論理和（K+ID）を用いる。このようにして公開のアルゴリズムと公開のIDを用いて秘密の暗号化が行われる。

【０００８】しかし、このようなデバイスバインドの著作権保護方式においては記録型メディアに記録されたコンテンツは記録した機器のみで再生でき、別の再生機では再生できないという欠点がある。記録型光ディスクのようにメディアが可搬性を持つ場合、この特性は、記録型メディアの可搬性を損なうものとなる。

【０００９】そこで、別の種類の著作権保護システムが考案されている。これはメディアバインドと呼ばれるものであり、ある記録メディアにはその記録メディア固有のID(識別情報)が存在し、記録されるデジタルコンテンツはその固有IDに依存した暗号鍵で記録･再生されるというものである。ここで固有IDは通常のパソコンなどのような一般ユーザが入手できる機器ではコピーができないものとされる。このようにすると、仮に識別情報がIDAである記録メディア上のデータがパソコンなどにより識別情報がIDBである記録メディアに丸ごとコピーされたとしても、記録メディア上に格納されたコンテンツはIDAを基に作成された暗号鍵で暗号化されているため、識別情報がIDBである記録メディアに丸ごとコピーされたコンテンツを再生しようとすると、再生機ではIDBを基に作成された復号鍵で復号されるため、首尾よく復号ができない。従って実質的に不正コピーの被害が生じないことを意図するものである。

【００１０】図5はこの種の著作権保護システムとして知られているものである。同図において100は映画などのコンテンツがデジタル化された、デジタルコンテンツを暗号化する記録機器、200は記録機器100により暗号化されたコンテンツを記録する記録型メディア、300は記録型メディアに記録された暗号化コンテンツを読み出し復号してデジタルコンテンツを再生する再生機器である。記録機器100には鍵暗号鍵計算部101、コンテンツ鍵発生部102、コンテンツ鍵暗号部103、コンテンツ格納部104、コンテンツ暗号部105がある。記録型メディア200にはメディア固有情報記録部201、暗号化コンテンツ鍵記録部202、暗号化コンテンツ記録部203がある。メディア固有情報は記録型メディアの１つ１つに固有の情報であり、製造時に書き込まれ、一般ユーザはリードできるがライトはできないものであるとする。情報は例えば64ビットの一連番号である。再生機器300には、鍵復号鍵計算部301、コンテンツ鍵復号部302、コンテンツ鍵一時格納部303、コンテンツ復号部304、デジタルAV処理回路305が備わる。

【００１１】この従来の著作権保護システムの動作の一例を示す。記録機器100には外部より、記録型メディアに暗号化記録すべきデジタルコンテンツが入力され、コンテンツ格納部104に格納されているものとする。記録

機器100に記録型メディア（例えば記録型光ディスク）が装着されたとき、記録型メディアのメディア固有情報記録部101よりメディア固有情報を読み出す。

【００１２】鍵暗号鍵計算部は、メディア固有情報を入力とし、秘密のデータを作成するためのものであり、一例として図６に図示する一方向性関数により実現される。図６において、400はDES暗号部、401は全ての記録機器および再生機器に共通の秘密であるマスター鍵、402は64ビットのビット毎の排他的論理和回路である。入力Aに64ビットのデータが入力された場合、DES暗号部400においてマスター鍵を鍵として暗号化が行われ、この結果が排他的論理和回路402において入力値とビット毎の排他的論理演算が行われる。その結果Bは後述するコンテンツ鍵の暗号鍵として用いられる。

【００１３】コンテンツ暗号鍵の暗号化の暗号アルゴリズムの一例としてDES暗号が用いられる場合、コンテンツ鍵発生部102が起動された場合、56ビットのランダムデータを生成する。このコンテンツ鍵はコンテンツ鍵暗号部103において上記コンテンツ鍵暗号鍵を用いてDES暗号化される。その結果である暗号化コンテンツ鍵は６４ビットであり、記録型メディア200の暗号化コンテンツ鍵記録部202に記録される。

【００１４】コンテンツ暗号化の暗号アルゴリズムの一例としてDES暗号が用いられる場合、コンテンツ格納部104に記録されているデジタルコンテンツは64ビットずつのブロックに区切られ、各ブロックのデータはコンテンツ暗号部205においてコンテンツ鍵発生部102の発生したコンテンツ鍵を用いて暗号化される。各ブロックが暗号化された結果が連結されてできた暗号化コンテンツは記録型メディア200の暗号化コンテンツ記録部203に記録される。

【００１５】再生機器300において、記録型メディア200が挿入されたとき、まず、鍵復号鍵計算部301は、記録型メディアのメディア固有情報記録部201よりメディア固有情報を読み出し、これを図６に図示する一方向性関数の入力として、その出力をコンテンツ鍵復号鍵データとして取り出す。ここで暗号アルゴリズムであるDES暗号および暗号鍵であるマスター鍵が、記録機器100の鍵暗号鍵計算部101のものと全く同一であれば、同じメディア固有情報を用いた場合、鍵復号鍵計算部301の出力は鍵暗号鍵計算部101の出力と同じ値になる。このことは共通鍵暗号であるDES暗号により暗号化されたデータを復号して元のデータを取り出すには必要である。

【００１６】再生機器300のコンテンツ鍵復号部302は記録型メディア200の暗号化コンテンツ鍵記録部202より暗号化コンテンツ鍵を読み出し、鍵復号鍵計算部301が生成したコンテンツ鍵復号鍵を用いて復号する。復号アルゴリズムはDESの復号アルゴリズムが用いられる。その出力はコンテンツ鍵一時格納部303に一時格納される。

【００１７】再生機器300のコンテンツ復号部304は記録

型メディア200の暗号化コンテンツ記録部203より暗号化コンテンツを読み出し、これを64ビットのブロックに区切り、これを入力としてコンテンツ復号部304においてコンテンツ鍵一時格納部303に一時格納されているコンテンツ鍵を用いて復号する。各ブロックに対する復号結果を連結したコンテンツデータは、デジタルAV処理回路305を介してアナログ音声画像データに変換され、スピーカやディスプレイによって出力されてユーザに視聴される。

【００１８】メディア固有情報IDAのメディアに記録された暗号化コンテンツ鍵と暗号化コンテンツを、メディア固有情報IDBのメディアにコピーした場合、このIDBのメディアを再生機器に装着したとき、鍵復号鍵計算部301が生成するタイトル復号鍵は、このコンテンツを本来記録したときに用いられた、IDAから導出される値とは異なる。従ってコンテンツ鍵復号部302の出力するコンテンツ鍵も本来の値とは異なる。従って、コンテンツ復号部304の出力は本来のものとは全く異なるものとなる。従ってデジタルAV処理回路305の出力からは本来の音楽や映像は出力されない。このようにしてメディアからメディアへのコピーに対する保護が実現される。

【００１９】

【発明が解決しようとする課題】しかしながら、上述した図5の構成の従来の著作権保護システムでは、復号されたコンテンツ鍵が本来正しいものであるか否かのチェックが全く行われない。従って、不正にコピーされた記録型メディアが装着されたときに、復号結果のコンテンツ鍵は暗号化に用いたものとは異なったものなり、この値で復号したコンテンツは意味のない全くランダムなデータになる。従って、コンテンツ復号の先立って確実にアラームを鳴らすなどユーザの注意を喚起するための措置をとることが困難であった。

【００２０】本発明はこれらの問題を解決するため、再生装置において復号して得られたコンテンツ鍵が本来あるべき値であるかどうかを確実に検査する仕組みを持たせた著作権保護システムを実現することを目的としている。

【００２１】

【課題を解決するための手段】上記目的を達成するために、請求項１の発明にかかわる著作権保護システムは、デジタルコンテンツを暗号化し暗号化コンテンツとして後述する記録型メディアに記録する記録機器と、メディア固有情報により一意的に識別され暗号化コンテンツを記録する記録型メディアと、記録型メディアに格納されている暗号化コンテンツを読み出して復号化しコンテンツを取り出して再生する再生機器からなり、上記記録機器は記録機器および再生機器に共通の秘密であるマスター鍵と、デジタルコンテンツを暗号化するときに用いるコンテンツ鍵と、上記マスター鍵でコンテンツ鍵を暗号化し暗号化コンテンツ鍵を作成するコンテンツ鍵暗号部

と、デジタルコンテンツを上記コンテンツ鍵を用いて暗号化し暗号化コンテンツを作成するコンテンツ暗号部と、記録型メディアから読み出したメディア固有情報と、上記マスター鍵と、上記コンテンツ鍵とを入力とする一方向性関数値を計算して許諾情報とする許諾情報計算部と、上記暗号化コンテンツ鍵と上記暗号化コンテンツと上記許諾情報を記録型メディアに記録する書き込み部を備え、上記記録型メディアは上記許諾情報と上記暗号化コンテンツ鍵と上記暗号化コンテンツを記録し、上記再生機器は、記録型メディアより暗号化コンテンツ鍵と暗号化コンテンツと許諾情報を読み出す読み出し部と、記録機器および再生機器に共通の秘密であるマスター鍵と、記録型メディアから読み込んだ暗号化コンテンツ鍵を上記マスター鍵を用いて復号しコンテンツ鍵を出力するコンテンツ鍵復号部と、記録型メディアから読み出したメディア固有情報と、上記マスター鍵と、上記コンテンツ鍵を入力として上記一方向性関数値を計算して参照許諾情報を作成する参照許諾情報計算部部と、参照許諾情報と、記録型メディアから読み出した許諾情報を比較し、一致したときのみディスクから読み出した暗号化コンテンツを上記コンテンツ鍵を用いて復号を行ってコンテンツを取り出すことを特徴とする。

【００２２】また、請求項２の発明にかかわる著作権保護システムは機器固有鍵を保持し、デジタルコンテンツを暗号化し後述する記録型メディアに記録する記録機器と、メディア固有情報により一意的に識別され暗号化デジタルコンテンツを記録する記録型メディアと、機器固有鍵を保持し、記録型メディアに格納されている暗号化コンテンツを読み出して復号化しコンテンツを取り出す再生機器からなり、上記記録型メディアはさらに、記録型メディアに付随するメディア鍵と機器固有鍵と機器無効化情報から設定されるメディア鍵データを予め記録し、上記記録機器はさらに、記録型メディアから上記メディア鍵データを読み出し、機器固有鍵を用いてメディア鍵を取り出すメディア鍵計算部と、デジタルコンテンツを暗号化するときに用いるコンテンツ鍵と、上記メディア鍵でコンテンツ鍵を暗号化し暗号化コンテンツ鍵を作成するコンテンツ鍵暗号部と、デジタルコンテンツを上記コンテンツ鍵を用いて暗号化し暗号化コンテンツを作成するコンテンツ暗号部と、記録型メディアから読み出したメディア固有情報と、上記メディア鍵と、上記コンテンツ鍵とを入力とする一方向性関数値を計算して許諾情報とする許諾情報計算部部と、上記暗号化コンテンツ鍵と上記暗号化コンテンツと上記許諾情報を記録型メディアに記録する書き込み部を備え、上記記録型メディアはさらに、許諾情報と暗号化コンテンツ鍵と暗号化コンテンツを記録し、上記再生機器はさらに、記録型メディアから上記メディア鍵データを読み出し、機器固有鍵を用いてメディア鍵を取り出すメディア鍵計算部と、記録型メディアよりメディア固有情報と、メディア鍵データと、暗号化コンテンツ鍵と暗号化コンテンツと許諾情報を読み出す読み出し部と、記録型メディアから読み込んだ暗号化コンテンツ鍵を上記メディア鍵を用いて復号しコンテンツ鍵を出力するコンテンツ鍵復号部と、記録型メディアから読み出したメディア固有情報と、上記メディア鍵と、上記コンテンツ鍵を入力として上記一方向性関数値を計算して参照許諾情報を作成する参照許諾情報計算部と、参照許諾情報と、記録型メディアから読み出した許諾情報を比較し、一致したときのみディスクから読み出した暗号化コンテンツを上記コンテンツ鍵を用いて復号を行ってコンテンツを取り出すことを特徴とする。

【００２３】また、請求項３の発明にかかわる著作権保護システムは、請求項２記載の著作権保護システムにおいて、メディア鍵データが、メディア鍵と機器固有鍵と、機器無効化情報から算出されるものであり、機器無効化情報に対応した機器固有鍵を保持している機器においては、前記メディア鍵計算部から前記メディア鍵が出力されないことを特徴とする。

【００２４】また、請求項４の発明にかかわる著作権保護システムは、暗号化コンテンツ鍵と暗号化コンテンツが、許諾情報とは異なるメディアに記録することを特徴とする。

【００２５】

【発明の実施の形態】（第１の実施形態）図１は請求項１の発明にかかわる著作権保護システムの一実施形態を示す図である。同図において10は映画や音楽などのコンテンツがデジタル化された、デジタルコンテンツを暗号化する記録機器、20は記録機器10により暗号化されたコンテンツを記録する記録型メディア、30は記録型メディア20に記録された暗号化コンテンツを読み出し復号してデジタルコンテンツを再生する再生機器である。記録機器10には記録機器および再生機器に共通の秘密であるマスター鍵11が秘密に格納されており、コンテンツの暗号に用いるコンテンツ鍵を発生するコンテンツ鍵発生部12、このコンテンツ鍵を暗号化するコンテンツ鍵暗号部13、暗号記録すべきコンテンツを格納しているコンテンツ格納部14、このコンテンツを暗号化するコンテンツ暗号部15、再生機器においてコンテンツの復号を許諾するかどうかの情報を担う許諾情報を計算する許諾情報計算部16がある。記録型メディア20にはメディア固有情報を記録するメディア固有情報記録部21、上記許諾情報を記録する許諾情報記録部22、上記暗号化コンテンツ鍵を記録する暗号化コンテンツ鍵記録部22、上記暗号化コンテンツを記録する暗号化コンテンツ記録部23がある。ここでメディア固有情報は記録型メディアの１つ１つに固有の情報であり、製造時に書き込まれ、一般ユーザはリードできるがライトはできないものであるとする。情報は例えば64ビットの一連番号である。再生機器300には、記録機器および再生機器に共通の秘密であるマスター鍵

31、暗号化コンテンツ鍵を復号するコンテンツ鍵復号部32、復号されて得られたコンテンツ鍵を一時格納するコンテンツ鍵一時格納部33、上記コンテンツ鍵で暗号化コンテンツを復号するコンテンツ復号部34、その結果であるデジタルコンテンツデータをAVデータとみなして所定の音声映像処理を行うデジタルAV処理回路35、参照のための許諾情報を計算する参照許諾情報計算部36、参照許諾情報と許諾情報を比較する比較部37、第1のスイッチ38、第2のスイッチ39、アラーム装置40が備わる。

【００２６】次にこの構成の第1の実施形態の動作の一例を説明する。記録機器10には外部より、記録型メディアに暗号化記録すべきデジタルコンテンツが入力され、コンテンツ格納部14に格納されているものとする。このような例としては例えば、デジタル衛星放送により放送されたデジタル映画コンテンツが衛星放送受信装置において受信し、デジタルコンテンツデータを記録機器により記録する場合がある。

【００２７】記録機器の制御回路（図示せず）はコンテンツ鍵発生部12に対して起動信号を出力する。このときコンテンツ鍵発生部12は、コンテンツ鍵として１つのランダムデータ（56ビット）を生成する。このコンテンツ鍵はコンテンツ鍵暗号部103においてマスター鍵11を用いて暗号化される。この暗号アルゴリズムの一例としてはDES暗号が用いられる。その結果である暗号化コンテンツ鍵は６４ビットであり、記録型メディア200に暗号化コンテンツ鍵記録部23に記録される。

【００２８】コンテンツ格納部14に記録されているデジタルコンテンツは64ビットずつのブロックに区切られ、各ブロックのデータはコンテンツ暗号部25においてコンテンツ鍵発生部12の発生したコンテンツ鍵を用いて暗号化される。このコンテンツ暗号アルゴリズムの一例としてはDES暗号が用いられる。各ブロックが暗号化された結果が連結されてできた暗号化コンテンツは記録型メディア20の暗号化コンテンツ記録部24に記録される。

【００２９】記録機器10に記録型メディア（例えば記録型光ディスク）が装着されたとき、記録機器10は記録型メディア20のメディア固有情報記録部11よりメディア固有情報を読み出す。許諾情報計算部16は、メディア固有情報とマスター鍵11とコンテンツ鍵を入力とし、許諾情報を作成するためのものであり、一例としてハッシュ関数SHA1により実現される。ハッシュ関数の入力Aはメディア固有情報64ビットとマスター鍵56ビットとコンテンツ鍵56ビットの連結であり、出力は160ビットである。この出力は許諾情報として記録型メディア20の許諾情報記録部22に記録される。

【００３０】再生機器30において、記録型メディア20が挿入されたとき、再生機器30のコンテンツ鍵復号部32は記録型メディア20の暗号化コンテンツ鍵記録部23より暗号化コンテンツ鍵を読み出し、マスター鍵格納部31に格納されているマスター鍵を用いて復号する。復号アルゴ

リズムはDESの復号アルゴリズムが用いられる。その出力はコンテンツ鍵一時格納部33に一時格納される。

【００３１】さらに、再生機器30は記録型メディア20のメディア固有情報格納部21からメディア固有情報を読み出し、これと、マスター鍵格納部31に格納されているマスター鍵と、コンテンツ鍵一時格納部33に格納されているコンテンツ鍵の連結を取り、これを参照許諾情報計算部36の入力とする。これに対して参照許諾情報計算部36は一方向関数SHA1の演算を行い、その結果の160ビットのデータを比較部37に対して出力する。比較部の他の一方の入力には記録型メディア20の許諾情報記録部22に記録されている許諾情報を読み出さした結果が入力される。そして比較部は２つの入力データが一致するかどうかを検査する。

【００３２】比較結果が一致した場合、第1のスイッチ38はONとなり、第2のスイッチはOFFとなる。このとき再生機器30のコンテンツ復号部34は記録型メディア20の暗号化コンテンツ記録部23より暗号化コンテンツを読み出し、これを64ビットのブロックに区切り、これを入力としてコンテンツ鍵一時格納部33に一時格納されているコンテンツ鍵を用いて復号する。各ブロックに対する復号結果を連結したコンテンツデータは、デジタルAV処理回路35を介してアナログ音声画像データに変換され、スピーカやディスプレイによって出力されてユーザに視聴される。

【００３３】一方、比較結果が一致しない場合、第1のスイッチはOFFとなり、第2のスイッチはONとなる。このときアラーム装置40が作動し、記録型メディアの読み出しにおいて不都合があったことをユーザに注意を喚起する。このときにはコンテンツ復号部34は復号動作を行わず、デジタルAV処理回路は映像音声出力を行わない。

【００３４】また、機器に対する物理的な攻撃により注意を払った実施形態においては、このよに比較結果が一致しない場合、コンテンツ鍵一時格納部33に格納されているコンテンツ鍵が消去される。また、ある一定回数以上のアラームが作動した場合、記録型メディアの該当するコンテンツにその旨の印をつけ、再生機器にはこの印の有無を検査する回路を設け、記録されたそのコンテンツがこれ以降利用不可となるような構成も可能である。

【００３５】以上のように、第1の実施形態においては、再生機器において、メディア固有情報と、マスター鍵と、コンテンツ鍵の３つの連結と、記録型メディアに記録されている許諾情報との整合性が検査される。従って、あるメディアに記録したコンテンツを別のメディアにコピーしても、メディア固有情報がコピーできないという特性のために、コピーされたコンテンツが首尾よく再生されることがなく著作物コンテンツの著作権を保護することができる。しかも従来にない特徴として検査に合格したときにのみコンテンツを復号したり、検査で不合格であった場合にアラームを鳴動させることができ

る。

【００３６】この第1の実施形態では、各記録機器および再生機器に共通の秘密の鍵であるマスター鍵が格納されていると仮定していた。しかし、ある１つの機器への物理的な攻撃があって本来秘密にされている内部が解析されて秘密情報が暴露された場合の他の機器への影響を考えると、マスター鍵を機器内に常に格納しておくのは好ましくない。そこで次に述べる第2の実施形態では、機器ごとに固有の鍵を用いて、正しい機器のみがこれを用いて前記マスター鍵と同様、共通の秘密鍵であるメディア鍵を計算して機器内に一時格納できる方法を述べる。

【００３７】（第２の実施形態）図2は請求項2の発明にかかわる著作権保護システムの一実施形態を示す図である。同図において60は映画などのコンテンツがデジタル化された、デジタルコンテンツを暗号化する記録機器、70は記録機器60により暗号化されたコンテンツを記録する記録型メディア、80は記録型メディア70に記録された暗号化コンテンツを読み出し復号してデジタルコンテンツを再生する再生機器である。記録機器60にはコンテンツ鍵発生部12、コンテンツ鍵暗号部13、コンテンツ格納部14、コンテンツ暗号部15、許諾情報計算部16がありこれらは第1の実施形態の同一の番号の構成要素と同じである。さらに記録機器60は、デバイス鍵17、メディア鍵計算部18、メディア鍵一時格納部19を有する。ここでデバイス鍵は記録機器固有の56ビットの秘密データである。メディア鍵計算部18は、後述する記録型メディア70のメディア鍵データを読み出し、これからメディア鍵を生成する装置である。その出力であるメディア鍵はメディア鍵一時格納部19に一時格納される。

【００３８】記録型メディア70にはメディア固有情報記録部21、許諾情報記録部22、暗号化コンテンツ鍵記録部22、暗号化コンテンツ記録部23がある。これらは第1の実施形態における同一の番号の構成要素と同じである。記録型メディア70にはさらにメディア鍵データ記録部25が備わる。これについて以下に説明する。

【００３９】メディア鍵データ記録部25にはメディア鍵データが記録される。メディア鍵データの一例を図３に示す。同図のようにメディア鍵データは8バイトのレコードの並びであり、各レコードはE(Kdi, Km)の形をしている。ここでEは暗号アルゴリズムであり；例えばDES暗号アルゴリズムが用いられる。Kdiはｉ番目のデバイス鍵を表す。ここでｉはデバイス（記録機器と再生機器を総称してデバイスと呼ぶ）の番号であり、この例ではデバイスには１から１２８までの番号が付けられている。Kdiは暗号鍵でありDES暗号の場合は５６ビットである。Kmは56ビットのメディア鍵である。Kmは記録型メディア70のある集合に対して一つ割り当てられるランダムな値である。ただし、後述の理由により０を除く。E(Kdi,Km)は、DES暗号を用いて、56ビットのメディア鍵を平文とし、56ビットのデバイス鍵を暗号鍵としてメディア鍵を暗号化した結果を意味している。メディア鍵データ記録部25は記録型メディア70において読み出しのみ可能領域の一部として実現される。第3レコードと第127レコードはE(Kdi,0)という記号が記されているが、これらのレコードは特別に、ゼロの値をデバイス鍵で暗号化したことを示している。このようにメディア鍵データを作ることによりKd3またはKd127をデバイス鍵として持つ機器ではメディア鍵Kmが得られず、正しくコンテンツの記録あるいは再生ができない。正確にいうと、これらの機器で記録したコンテンツを、他の正当な機器で再生できない。また、他の正当な機器で記録されたコンテンツをこれらの機器で再生することはできない。従って、このメディア鍵データによってそれらの機器を「無効化」することができる。あるいは、メディア鍵計算部の出力がゼロの値であることを検知して、記録あるいは再生の処理に入る前に、処理を中止して、エラー通知を出すようにすることも可能である。このメディア鍵データは、記録型メディアの製造時点で記録型メディアの読み出し専用領域に記録される。

【００４０】再生機器80には、コンテンツ鍵復号部32、コンテンツ鍵一時格納部33、コンテンツ復号部34、デジタルAV処理回路35、参照許諾情報計算部36、比較部37、第1のスイッチ38、第2のスイッチ39、アラーム装置40が備わる。これらは第1の実施形態の同一の番号の構成要素と同じである。さらに再生機器80は、デバイス鍵41、メディア鍵計算部42、メディア鍵一時格納部43を有する。ここでデバイス鍵41、メディア鍵計算部18およびメディア鍵一時格納部19と同じ機能を有する。

【００４１】次にこの構成の第2の実施形態の動作の一例を説明する。記録機器60には外部より、記録型メディアに暗号化記録すべきデジタルコンテンツが入力され、コンテンツ格納部14に格納されているものとする。

【００４２】記録機器60に記録型メディア（例えば記録型光ディスク）70が装着されたとき、記録機器60は記録型メディア70のメディア鍵データ記録部25よりメディア鍵データを読み出す。メディア鍵計算部18は、記録機器60に備わるデバイス番号記録部（図示せず）よりその記録機器のデバイス番号を読み取り、メディア鍵データのうちの該当のレコードを取り出す。そして、デバイス鍵17を復号鍵として復号する。該当のレコードはE(Kdi,Km)あるいはE(Kdi,0)であるから、これをKdiで復号すると、メディア鍵Kmあるいは0が得られる。この結果が０である場合には処理を中止する。０でない場合にはメディア鍵Kmをメディア鍵一時格納部19に一時格納する。メディア鍵が0である場合、その機器は無効化されていることを意味する。

【００４３】コンテンツ鍵発生部12が起動されると、１つのランダムデータ（56ビット）を生成する。このコンテンツ鍵はコンテンツ鍵暗号部13においてメディア鍵19

を用いて暗号化される。暗号アルゴリズムの一例としてはDES暗号が用いられる。その結果である暗号化コンテンツ鍵は６４ビットであり、記録型メディア70の暗号化コンテンツ鍵記録部23に記録される。

【００４４】コンテンツ格納部14に記録されているデジタルコンテンツは64ビットずつのブロックに区切られ、各ブロックのデータはコンテンツ暗号部15においてコンテンツ鍵発生部12の発生したコンテンツ鍵を用いて暗号化される。この暗号アルゴリズムの一例としてはDES暗号が用いられる。各ブロックが暗号化された結果が連結されてできた暗号化コンテンツは記録型メディア70の暗号化コンテンツ記録部24に記録される。

【００４５】また、記録機器60に記録型メディア（例えば記録型光ディスク）が装着されたとき、記録機器60は記録型メディア70のメディア固有情報記録部21よりメディア固有情報を読み出す。許諾情報計算部部16は、メディア固有情報とメディア鍵一時格納部19に一時格納されているメディア鍵Kmとコンテンツ鍵を入力とし、許諾情報を作成するためのものであり、一例としてハッシュ関数SHA1により実現される。ハッシュ関数の入力Aはメディア固有情報64ビットとメディア鍵56ビットとコンテンツ鍵56ビットの連結であり、出力は160ビットである。この出力は許諾情報として記録型メディア70の許諾情報記録部22に記録される。

【００４６】再生機器80に記録型メディア70が装着されたとき、再生機器80は記録型メディア70のメディア鍵データ記録部25よりメディア鍵データを読み出す。メディア鍵計算部42は、再生機器80に備わるデバイス番号記録部（図示せず）よりその記録機器のデバイス番号を読み取り、メディア鍵データのうちの該当のレコードを取り出す。そして、デバイス鍵41を復号鍵として復号する。該当のレコードはE(Kdi,Km)あるいはE(Kdi,0)であるから、これをKdiで復号すると、メディア鍵Kmあるいは0が得られる。この結果が０である場合には処理を中止する。メディア鍵が0である場合、その機器は無効化されていることを意味する。０でない場合にはメディア鍵Kmをメディア鍵一時格納部43に一時格納する。

【００４７】再生機器80において、記録型メディア70が挿入されたとき、再生機器80のコンテンツ鍵復号部32は記録型メディア70の暗号化コンテンツ鍵記録部23より暗号化コンテンツ鍵を読み出し、メディア鍵一時格納部43に格納されているメディア鍵を用いて復号する。復号アルゴリズムはDESの復号アルゴリズムが用いられる。その出力はコンテンツ鍵一時格納部33に一時格納される。

【００４８】さらに、再生機器30は記録型メディア70のメディア固有情報格納部21からメディア固有情報を読み出し、これと、メディア鍵一時格納部43に一時格納されているメディア鍵と、コンテンツ鍵一時格納部33に格納されているコンテンツ鍵の連結を取り、これを参照許諾情報計算部36の入力とする。これに対して参照許諾情報計算部部36は一方向関数SHA1の演算を行い、その結果の160ビットのデータを比較部37に対して出力する。比較部の他の一方の入力には記録型メディア70の許諾情報記録部22に記録されている許諾情報を読み出された結果が入力される。そして比較部は２つの入力データが一致するかどうかを検査する。

【００４９】比較結果が一致した場合、第1のスイッチ38をONにし、第2のスイッチをOFFにする。このとき再生機器80のコンテンツ復号部34は記録型メディア70の暗号化コンテンツ記録部24より暗号化コンテンツを読み出し、これを64ビットのブロックに区切り、これを入力としてコンテンツ復号部34においてコンテンツ鍵一時格納部33に一時格納されているコンテンツ鍵を用いて復号する。各ブロックに対する復号結果を連結したコンテンツデータは、デジタルAV処理回路35を介してアナログ音声画像データに変換され、スピーカやディスプレイによって出力されてユーザに視聴される。

【００５０】一方、比較結果が一致しない場合、一致しなければ第1のスイッチをOFFにし、第2のスイッチをONにする。このときアラーム装置40が作動し、記録型メディアの読み出しにおいて不都合があったことをユーザに注意を喚起する。このときにはコンテンツ復号部34は復号動作を行わず、デジタルAV処理回路は映像音声出力を行わない。

【００５１】このように、第2の実施形態においては、メディア鍵データを記録型メディアに記録し、メディア鍵計算部がこれを読み出してメディア鍵を生成するという構成をとったために、上記の効果が、メディア鍵の無効化効果と共に発揮される。

【００５２】第１および第2の実施形態において、不正にコピーされた記録型メディアを用いて再生を行った場合において、コンテンツ鍵格納部33にはコンテンツ復号部34においてコンテンツを復号するに十分な情報が格納されている。このデータはスイッチ38がONにならない限りコンテンツ復号部34には通知されることがないものであるが、機器内部の解析により不正が行われる危険性がある。第3の実施形態はこのことを考慮し、安全性をさらに向上した構成である。

【００５３】（第３の実施形態）第3の実施形態は、図４に示すように、第2の実施形態において、記録機器60において、コンテンツ鍵暗号部13に代えて第1のコンテンツ鍵暗号部131と第2のコンテンツ鍵暗号部132の直列の構成を備えたものである。いずれもメディア鍵を暗号鍵とする。従って、コンテンツ鍵はメディア鍵で２重にDES暗号化され、この結果が記録型メディア70の暗号化コンテンツ鍵記録部に格納される。一方、再生機器80において第2の実施形態におけるコンテンツ鍵復号部32の代わりに、第2のコンテンツ鍵復号部とし、スイッチ38とコンテンツ復号部34の間に第1のコンテンツ鍵復号部322を設けたものである。この構成ととると、第2のコン

テンツ鍵復号部321は記録型メディアに記録された、２重暗号化されたコンテンツ鍵をメディア鍵を用いて1度復号する。その結果はコンテンツ鍵が１重暗号化されたものになる。これがコンテンツ鍵一時格納部33に一時格納される。比較部において、参照許諾情報と許諾情報の一致が確認されたとき、スイッチ38がONになることにより、コンテンツ鍵一時格納部33に一時格納されていた1重暗号化されたコンテンツ鍵が第1のコンテンツ鍵復号部38の入力に入り、これがメディア鍵で復号化されてコンテンツ鍵が得られる。

【００５４】このように第3の実施形態においては、コンテンツ鍵一時格納部33に格納されるデータが、暗号化コンテンツを復号するのに十分な情報ではないために第1、第2の実施形態に比べ、機器が解析されたときの安全性がさらに向上する。

【００５５】許諾情報計算部が、メディア固有情報とメディア鍵とコンテンツ鍵を入力とする一方向性関数値である限り、上記構成以外の別の構成も可能である。

【００５６】なお、実施形態１および２において、コンテンツ鍵は記録機器で生成するものとして説明したが、本発明はこれの構成に限定されるものではなく、例えばコンテンツ製作者あるいは著作権保持者がコンテンツ鍵を決定し、これを安全な形で記録機器に配送され、記録機器に入力するものであってもよい。

【００５７】また、第1および第2の実施形態においてメディア固有情報、許諾情報、暗号化コンテンツ鍵、および暗号化コンテンツは１つの記録型メディアに記録されていたが、本発明はこれに限定されるものではなく、例えば暗号化コンテンツ鍵と暗号化コンテンツが、許諾情報が記録されるのとは異なる別メディアに記録されるという構成であってもよい。この別メディアはメディア固有情報に依存せずに求められため、例えば予め読み出し専用メディアで供給するというものであってもよい。また、第1の実施形態ではマスター鍵、第2の実施形態ではメディア鍵データを決定する装置と、コンテンツ鍵を決定して暗号化コンテンツ鍵と暗号化コンテンツを作成する装置はそれぞれ異なる装置に存在させることにより、２つの装置それぞれ単独ではコンテンツを再生するための情報が作成できないからより安全性が増加する。

【００５８】（その他の変形例）なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

【００５９】（１）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【００６０】また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ―ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【００６１】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

【００６２】また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【００６３】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【００６４】（２）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【００６５】

【発明の効果】本願発明（請求項１）にかかわる著作権保護システムは、記録機器は、記録型メディアから読み出したメディア固有情報と、マスター鍵と、上記コンテンツ鍵とを入力とする一方向性関数値を計算して上記許諾情報を記録型メディアに記録し、再生機器は、記録型メディアから読み出したメディア固有情報と、マスター鍵と、復号して得られたコンテンツ鍵を入力として一方向性関数値を計算して参照許諾情報を作成し、これと記録型メディアから読み出した許諾情報を比較し、一致したときのみディスクから読み出した暗号化コンテンツを上記コンテンツ鍵を用いて復号を行ってコンテンツを取り出すことができる。

【００６６】また、本願発明（請求項２）にかかわる著作権保護システムは、記録機器は、記録型メディアから読み出したメディア固有情報と、メディア鍵と、上記コンテンツ鍵とを入力とする一方向性関数値を計算して上記許諾情報を記録型メディアに記録し、再生機器は、記録型メディアから読み出したメディア固有情報と、メディア鍵と、復号して得られたコンテンツ鍵を入力として一方向性関数値を計算して参照許諾情報を作成し、これと記録型メディアから読み出した許諾情報を比較し、一致したときのみディスクから読み出した暗号化コンテンツを上記コンテンツ鍵を用いて復号を行ってコンテンツを取り出すことができる。

【００６７】また、本願発明（請求項３）にかかわる著作権保護システムは．機器無効化情報に対応した機器固有鍵を保持している機器、すなわち無効化された機器に

17

おいては、前記メディア鍵計算部から前記メディア鍵が出力されないために、無効化された機器で記録したコンテンツは無効化されていない正常な機器で読み出すことができず、一方、正常な機器で記録したコンテンツは無効化された機器で再生することができない。

【００６８】また、本願発明（請求項４）にかかわる著作権保護システムは,暗号化コンテンツ鍵と暗号化コンテンツを記録したメディアと、許諾情報を記録したメディアを独立に取り扱うことができる。

【図面の簡単な説明】

【図１】本発明の第1の実施形態の構成図

【図２】本発明の第2の実施形態の構成図

【図３】メディア鍵データの格納状態の一例を示す図

18

【図４】本発明の第3の実施形態の構成図

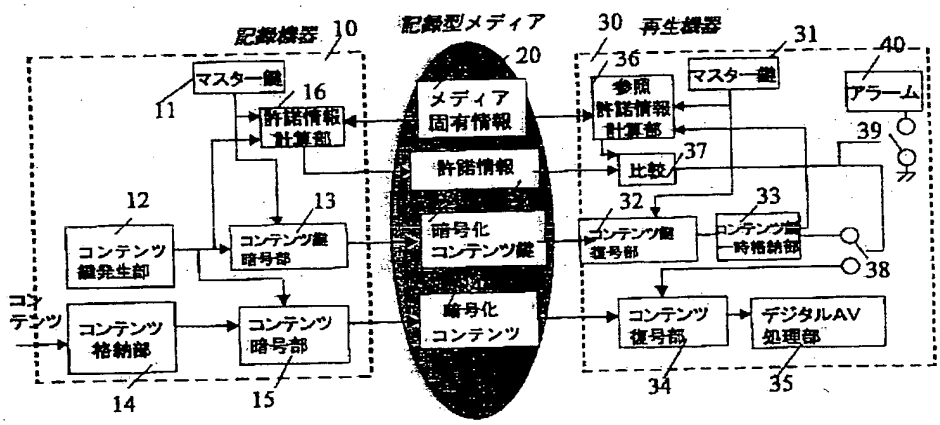
【図５】従来の著作権保護システムの構成図

【図６】鍵暗号鍵計算部の構成の一例を示す図

【符号の説明】

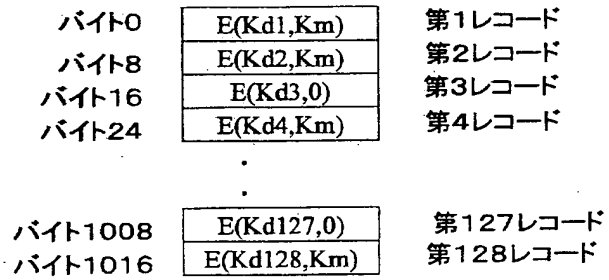
13　コンテンツ鍵暗号部
15　コンテンツ暗号部
16　許諾情報計算部
22　許諾情報記録部
32　コンテンツ鍵復号部
34　コンテンツ復号部
36　参照許諾情報計算部
37　比較部

【図１】



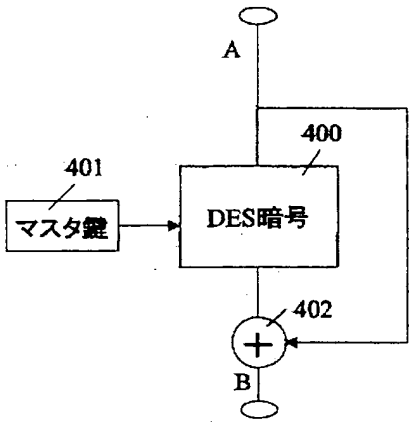
第１の実施例の構成図

【図３】



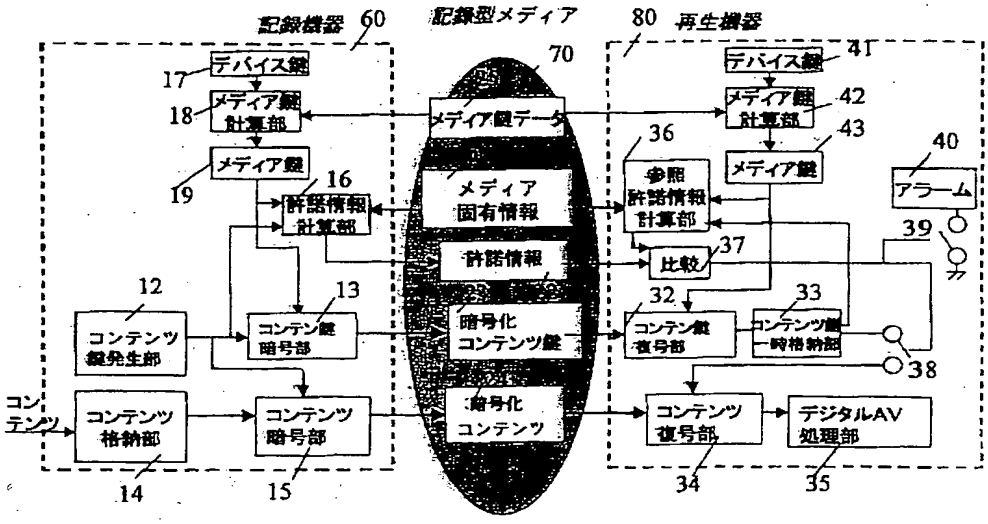
メディア鍵データ格納状態の一例

【図６】



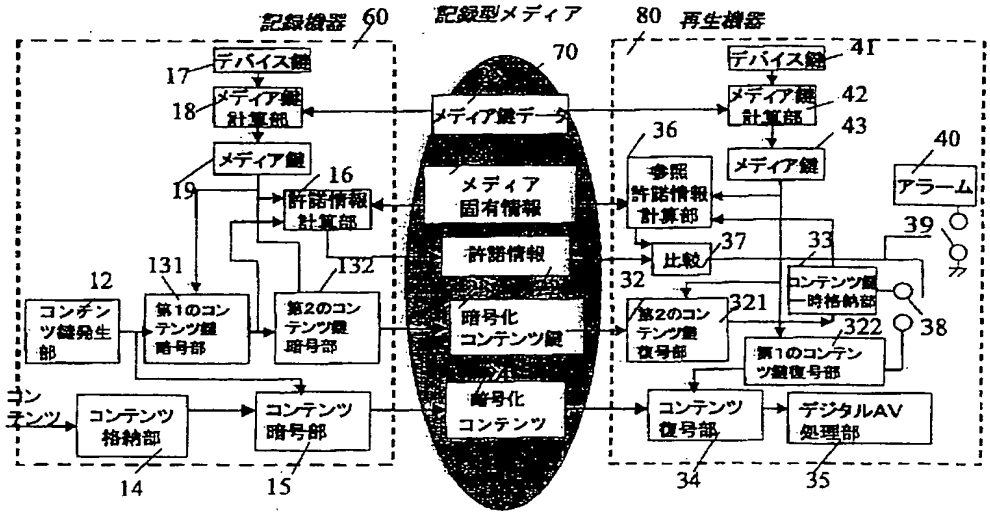
鍵暗号鍵計算部の構成の一例

【図２】



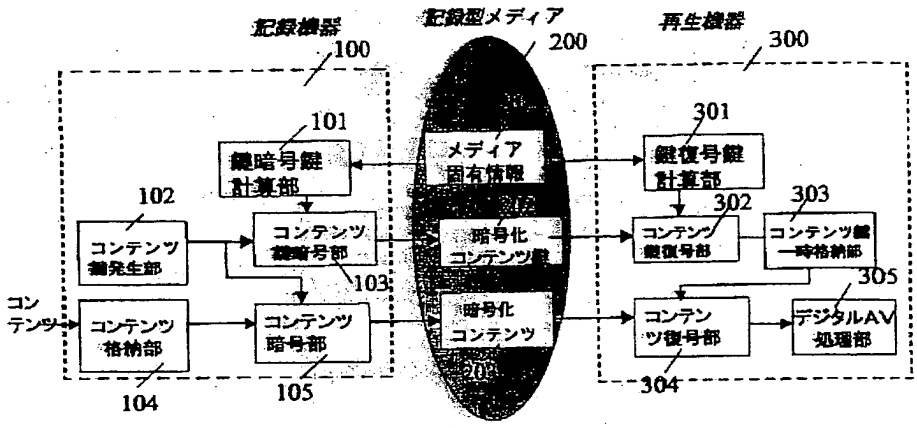
第２の実施例の構成図

【図４】



第３の実施例の構成図

【図５】



従来の著作権保護システムの構成図

フロントページの続き

(72)発明者　原田　俊治
大阪府門真市大字門真1006番地　松下電器
産業株式会社内

Ｆターム(参考)　5B017 AA06 BA07 BA09 CA09 CA16
5J104 AA01 AA13 AA16 AA32 EA02
EA06 EA17 NA03 PA14